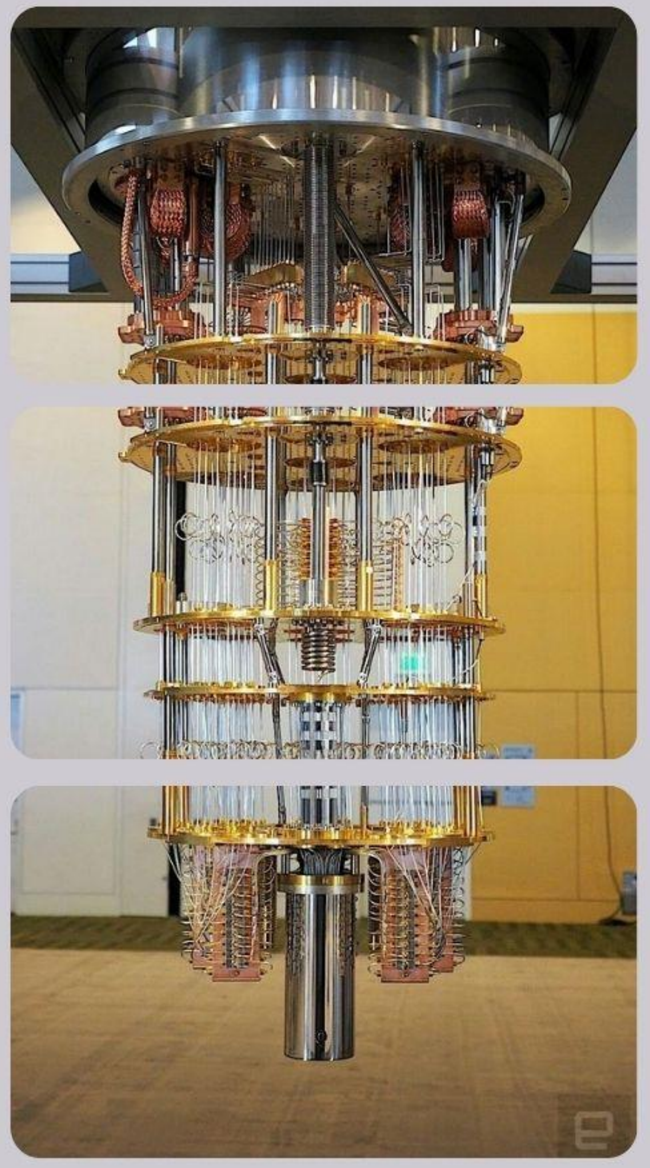
UNDERSTANDING QUANTUM COMPUTING

WARNING

Contains Quantum Physics & Math. May Cause Brain Overload! Proceed with Caution.



WHAT IS A QUANTUM COMPUTER?

A Quantum Computer is a device that leverages the principles of **quantum mechanics**, such as **superposition** and **entanglement**, to perform complex operations much faster and more efficiently.

HOW IS DATA STORED?

▶▶ CLASSICAL COMPUTERS

- Data is stored in bits.
- Each bit is either a 0 or a 1.

▶▶ QUANTUM COMPUTERS

- Data is stored in qubits (typically subatomic particles, such as electrons or photons)

- Each qubit can be a 0, a 1, or both at the same time (thanks to a property called **superposition**).

- Qubits can also be **entangled**, meaning the state of one qubit is linked to the state of another, allowing for more complex data storage and processing.

HOW ARE QUBITS MANIPULATED?

- $|0\rangle$, $|1\rangle$ - states of a qubit. $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- Mixed state: $|+\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

Quantum operations – quantum gates perform operations on qubits to manipulate their states.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

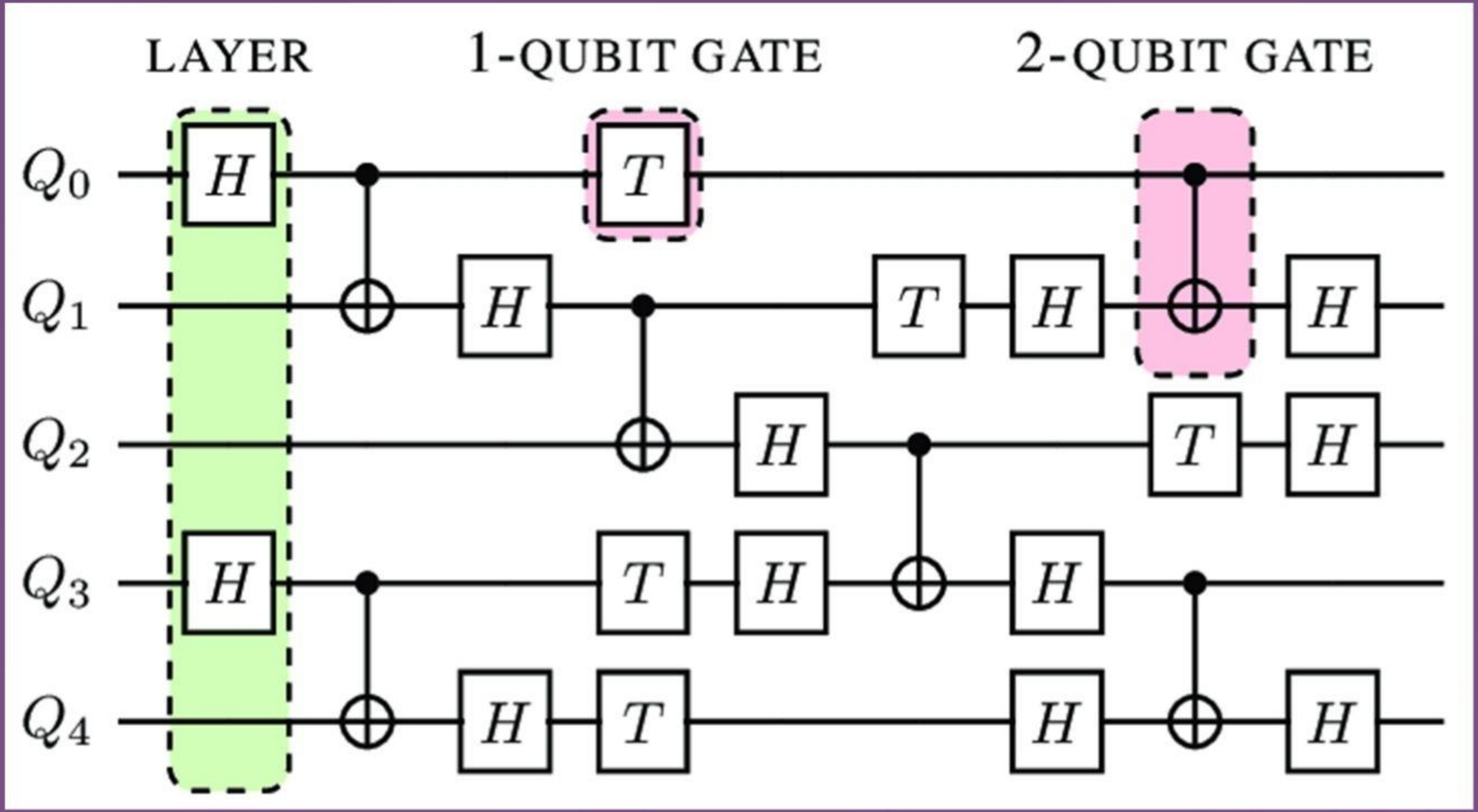
$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} (1 * 0) + (0 * 1) \\ (1 * 1) + (0 * 0) \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

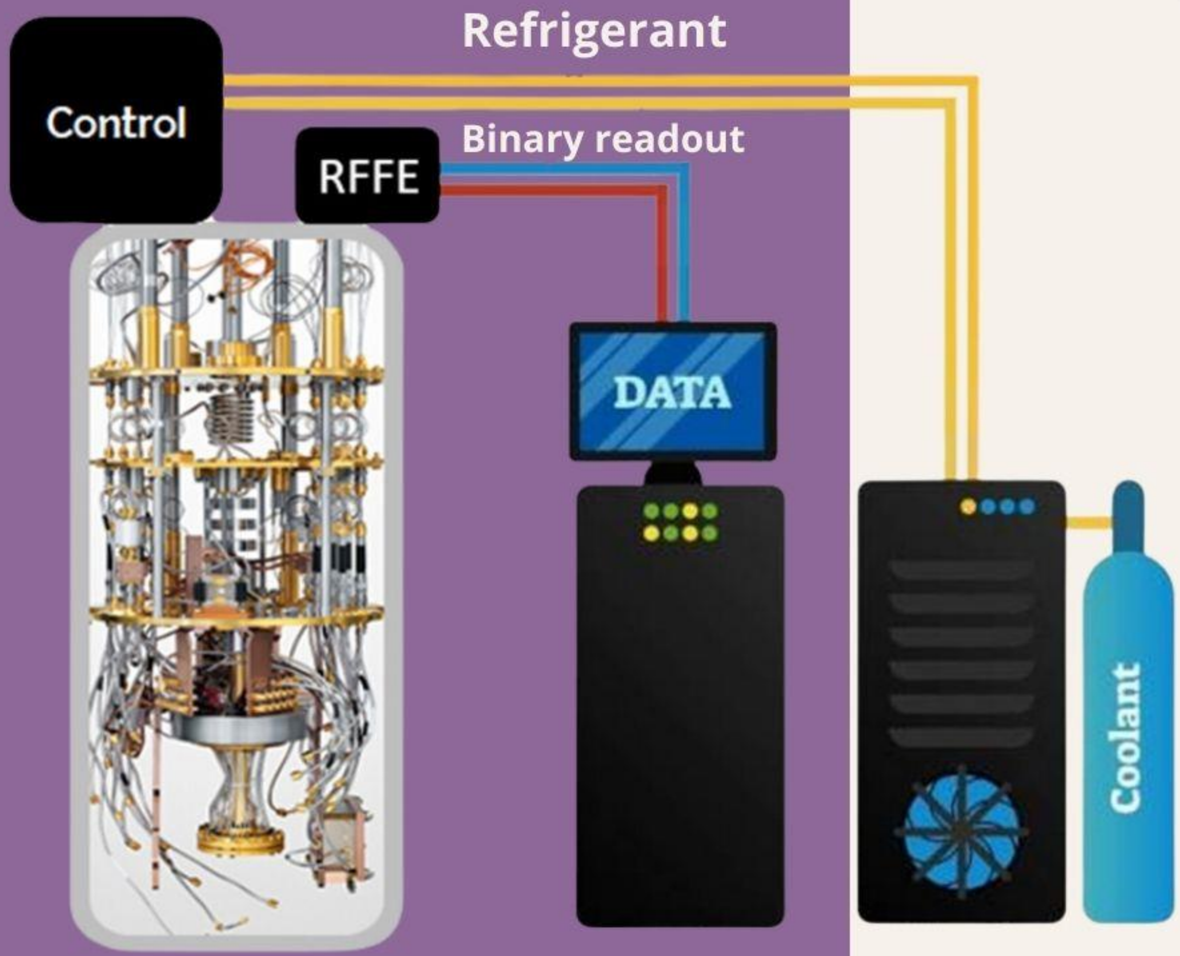
EXAMPLE OF A MEASUREMENT

$$\begin{tikzcd} & {|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}} \arrow[dl, "\frac{1}{2}"'] \arrow[dr, "\frac{1}{2}"] & \\ {|0\rangle} & & {|1\rangle} \end{tikzcd}$$

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

EXAMPLE OF A QUANTUM CIRCUIT





Parts of a Quantum Computer system

- **Quantum Processor (Left)**: performs quantum computations using qubits and different operations.
- **Control (Top Left)**: generates microwave pulses or laser beams used to control the qubit states. (sending signals in short)
- **RFFE (radio Frequency Front End)**: processes signals going to and coming from the qubits.
- **Data**: interprets the measurement results into classical data.
- **Coolant (Right)**: maintains the low temperatures required for quantum operations. It keep the quantum processor at temperatures close to absolute zero.

How is it different from super computers or mainframes?

01. Quantum Computers

- **Technology**: Quantum bits (qubits).
- **Strength**: Speed in solving specific complex problems.
- **Use Case**: Cryptography, quantum simulations.

03. Supercomputers

- **Technology:** Massive parallel processing with traditional CPUs/GPUs.
- **Strength**: General high-performance computing.
- **Use Case**: Scientific research, climate modeling, AI.

02 Mainframes

- **Technology**: Reliable and robust traditional processors.
- **Strength**: High reliability and transaction processing.
- **Use Case**: Banking, enterprise applications, large databases.

Why is it important?

A

Atoms Simulations

The real world runs on quantum physics. Classical computers can't accurately model the behavior of individual atoms in a molecule, but quantum computers can, as they leverage the principles of quantum physics.

B

AI Advancements

Quantum computers can significantly enhance artificial intelligence by solving complex optimization problems and processing vast amounts of data more efficiently, leading to faster and more accurate machine learning algorithms.

C

Cryptography

Quantum computers have the potential to break traditional encryption methods, necessitating the development of quantum-safe cryptography. They also enable the creation of new cryptographic algorithms that are fundamentally more secure.

D

Battery Development

Quantum computers can model and simulate the complex chemical reactions within batteries at an atomic level, leading to the design of more efficient and powerful energy storage solutions.

What is a relation between Quantum computers and Quantum-safe cryptography on mainframes?

Quantum-safe cryptography was developed to protect data against the potential threats posed by quantum computers.

RSA and Factoring-Based Cryptography

Vulnerable due to Shor's algorithm.

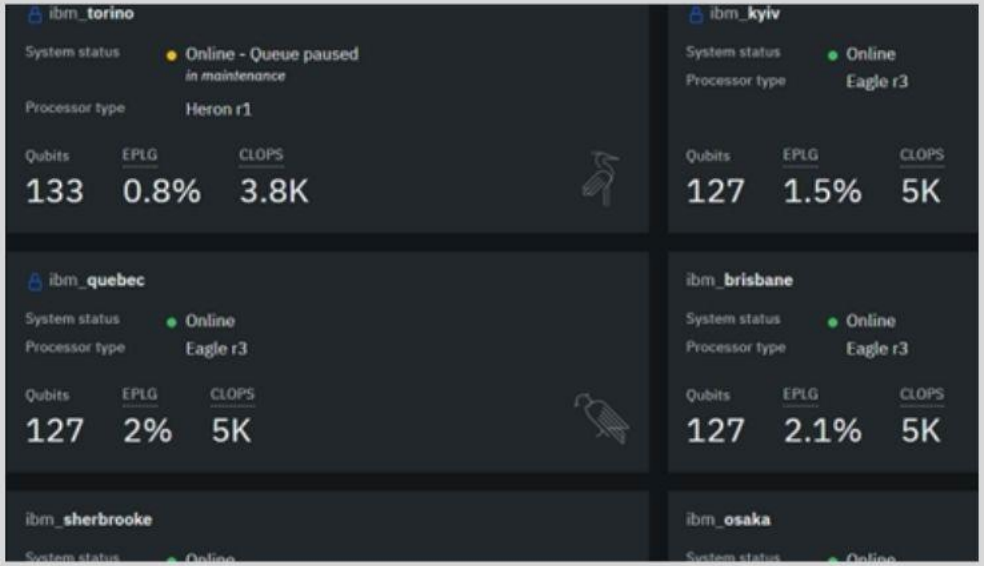
Diffie-Hellman and

Vulnerable due to Shor's algorithm solving discrete logarithms.

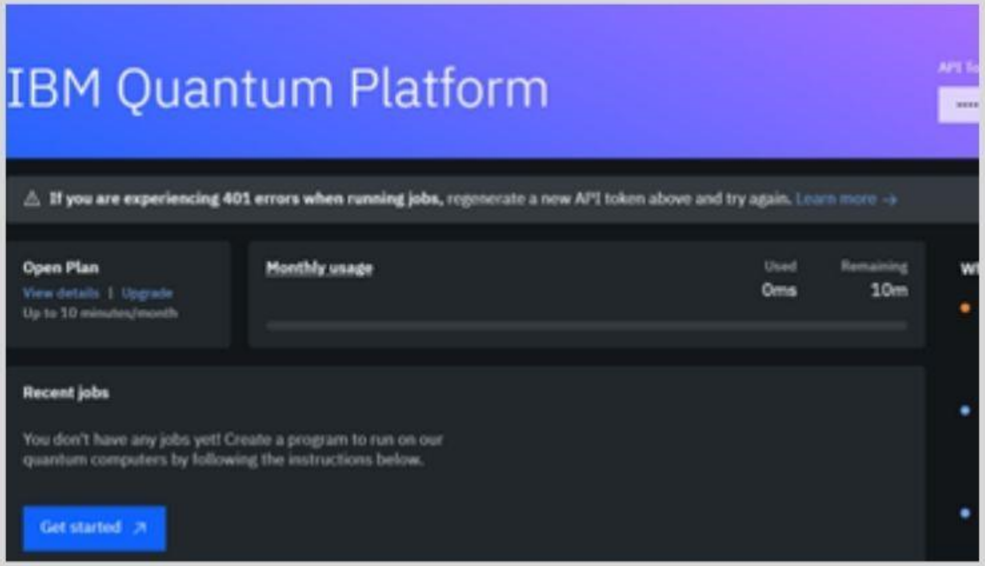
Symmetric-Key Cryptography

Weakened (but not broken) by Grover's algorithm.

HOW TO USE QUANTUM COMPUTATION ON OUR COMPUTERS?



Qiskit



IBM Quantum Challenge 2024

Lab 0

Building your first simple program using Qiskit.

Lab 1

Learning how to use different operators and seeing the power of quantum computation in practice by building a Variational Quantum Eigensolver (VQE).

Lab 2

Learning how to configure a transpiler and understanding how it works.

IBM Quantum Challenge 2024

Lab 3

Exploring upcoming features, such as the AI transpiler, Qiskit serverless, Code Assistant, and circuit knitting.

Lab 4

Using Qiskit to build a quantum classifier (machine learning).

PRACTICE TIME?